OULUN AMMATTIKORKEAKOULU

Juho Mäkelä

VERKON LAITTEIDEN VALVONTA

VERKON LAITTEIDEN VALVONTA

Juho Mäkelä
Opinnäytetyö
Syksy 2015
Tietojenkäsittely
Oulun ammattikorkeakoulu

TIIVISTELMÄ

Oulun ammattikorkeakoulu
Tietojenkäsittely, Järjestelmäasiantuntemus

Tekijä: Juho Mäkelä
Opinnäytetyön nimi: Verkon laitteiden valvonta
Työn ohjaaja: Pekka Ojala
Työn valmistumislukukausi- ja vuosi: Syksy 2015 Sivumäärä: 30

Opinnäytetyön tavoitteena oli toteuttaa verkonvalvontajärjestelmä oululaiselle ICT-alan yritykselle. Järjestelmän avulla oli tarkoitus valvoa yrityksen verkossa olevien laitteiden tilaa ja pitää kirjaa verkon laitteista. Ratkaisun tuli olla mahdollisimman kustannustehokas, joten toteutuksessa käytettiin maksuttomia avoimen lähdekoodin ohjelmistoja.

Järjestelmä toteutettiin käyttäen CentOS Linux-käyttöjärjestelmää sekä Observium- ja OCS Inventory NG -ohjelmistoja. Observiumin avulla valvotaan verkon laitteiden, kuten kytkimien ja palvelimien tilaa. OCS Inventory NG:n avulla taas pidetään kirjaa verkossa olevista työasemista sekä niiden laitteistosta ja asennetuista ohjelmista.

Työn teoriaosuudessa käsitellään verkonhallintaa ja -valvontaa sekä perehdytään SNMP-protokollaan, joka on yleisin verkonhallinnassa käytetty protokolla. Verkonhallinnan merkittävimmät osa-alueet käydään läpi ja kerrotaan verkonhallinnan toteuttamisesta. SNMP-protokollan toiminta selitetään ja vertaillaan hieman sen eri versioita.

Asiasanat: verkonhallinta, verkonvalvonta, SNMP

ABSTRACT

Oulu University of Applied Sciences
Degree Programme in Information Systems, Computer Systems Expertise

---

Author: Juho Mäkelä
Title of thesis: Network device monitoring
Supervisor(s): Pekka Ojala
Term and year when the thesis was submitted: Autumn 2015 Number of pages: 30

The aim of this thesis was to implement a network monitoring system for an ICT company located in Oulu, Finland. The system was intended to monitor and keep record of the company's network equipment. The system had to be implemented cost-effectively, so it was decided to use free open source software.

The system was implemented using CentOS Linux operating system as well as Observium and OCS Inventory NG software. Observium allows the administrator to monitor the status of network devices such as switches and servers. OCS Inventory NG keeps track of the workstations on the network along with their hardware and installed software.

The theoretical background of the thesis deals with network management and monitoring. The most significant areas of network management are reviewed. It also focuses on the most common network management protocol SNMP. Protocol operation is explained and the protocol versions are slightly compared.

Keywords: network management, network monitoring, SNMP

SISÄLLYS

1 JOHDANTO

Opinnäytetyön toimeksiantaja oli oululainen ICT-alan yritys. Tarkoituksena oli toteuttaa yritykselle järjestelmä, jonka avulla voitaisiin valvoa sen verkossa olevien laitteiden tilaa ja pitää kirjaa verkon laitteista. Idea opinnäytetyöhön syntyi ollessani kesätöissä kohdeyrityksessä.

Toimeksiantajan verkossa oli noin 100 työasemaa, palvelimia, palomuuri, kytkimiä ja paljon muita laitteita. Verkossa olevien laitteiden määrä oli myös jatkuvasti kasvussa ja näinkin suurta verkkoa oli jo vaikea valvoa ihmisvoimin. Yrityksessä oli siis tarve automatisoidulle verkonvalvontajärjestelmälle. Järjestelmä haluttiin luonnollisesti toteuttaa mahdollisimman pienillä kustannuksilla, joten päätettiin käyttää maksuttomia avoimen lähdekoodin ratkaisuja. Ennakkoselvitysten perusteella käytettäviksi valvontaohjelmistoiksi oli valittu Observium ja OCS Inventory NG, jotka asennettiin CentOS Linux-jakeluun.

Opinnäytetyön teoriaosuudessa käsitellään verkonhallintaa ja -valvontaa sekä perehdytään SNMP-protokollaan, joka on yleisin verkonhallinnassa käytetty protokolla. Verkonhallinnan merkittävimmät osa-alueet käydään läpi ja kerrotaan verkonhallinnan toteuttamisesta. SNMP-protokollan toiminta selitetään ja vertaillaan hieman sen eri versioita. Lopuksi asennettavat ohjelmistot esitellään ja niiden asennuksen vaiheet käydään läpi pääpiirteittäin.

2 VERKONHALLINTA

Yhä useamman henkilön, ja samalla yrityksen, tuottavuus ja työn tehokkuus ovat riippuvaisia hyvin toimivasta verkosta. Verkko ja siihen liitetyt laitteet ovat osa yrityksen toiminnallista ympäristöä ja verkon toiminnan häiriintyminen näkyy välittömästi yrityksen toiminnan tasossa. Nykyään lähes jokainen keskisuuri tai suuri yritys toimii erilaisten tietojärjestelmien varassa, ja jo muutaman tunnin keskeytys tietojärjestelmien toiminnassa voi aiheuttaa yritykselle huomattavaa vahinkoa. Sen lisäksi, että viallinen verkko usein tuottaa ylimääräisiä kustannuksia yritykselle, se tuottaa vaivaa verkosta vastuussa olevalle henkilölle tai osastolle. Vikoja ja häiriöitä on pystyttävä ennaltaehkäisemään ja niihin on voitava puuttua välittömästi niiden ilmaannuttua. (Jaakohuhta & Lahtinen 1997, 493.)

Tarve verkonhallinnalle näkyy selvästi jo muutaman kymmenen työaseman verkoissa, mutta korostuu entisestään suuremmissa verkoissa. Yleensä suurissa verkoissa on työasemien lisäksi myös useita muita erityyppisiä laitteita useilta eri valmistajilta. Tällaisia suuria ja monimutkaisia verkkoja ei enää pystytä hallitsemaan pelkästään ihmisvoimin, vaan tarvitaan automatisoituja ja standardoituja verkonhallintatyökaluja. (Jaakohuhta & Lahtinen 1997, 493–494.)

2.1 Verkonhallinnan osa-alueet

ISO:n (International Organization for Standardization) OSI-järjestelmänhallinnassa verkonhallinta on jaettu osa-alueisiin. Tämä jako on saavuttanut laajan hyväksynnän myös muiden verkonhallintajärjestelmien kuvauksessa. ISO:n määrittelemät verkonhallinnan avainalueet ovat:

- Vikojen hallinta (Fault management)
- Käytön hallinta (Accounting management)
- Kokoonpanon hallinta (Configuration management)
- Suorituskyvyn hallinta (Performance management)
- Turvallisuuden hallinta (Security management)

  (Jaakohuhta & Lahtinen 1997, 495–496.)

2.1.1 Vikojen hallinta

Monimutkaisen verkon toiminnan ylläpitämiseksi on huolehdittava, että järjestelmä kokonaisuutena ja sen jokainen olennainen laite itsessään on toimintakunnossa. Kun verkon vikaantuminen havaitaan, on paikallistettava täsmällisesti, missä vika on, ja eristettävä muu verkko vian aiheuttamilta häiriöiltä. Verkkoa on muutettava tai konfiguroitava siten, että minimoidaan vian vaikutukset verkon toimintaan ilman vikaantunutta laitetta. Vikaantunut laite on korjattava tai vaihdettava verkon palauttamiseksi normaaliin tilaansa. Kun vika on korjattu ja verkko on taas toimintakunnossa, on varmistuttava, että ongelma on todellakin ratkaistu eikä uusia ongelmia ole syntynyt. (Jaakohuhta & Lahtinen 1997, 496–497.)

Vikojen hallinta antaa ylläpitäjille työkalut, joiden avulla saadaan tietoa verkon kunkin hetkisestä tilasta. Parhaimmillaan nämä työkalut kertovat tarkasti, milloin vika on syntynyt ja ilmoittavat siitä välittömästi ylläpitäjälle. Verkon luotettavuus paranee, kun viat voidaan havaita nopeasti ja ryhtyä heti toimenpiteisiin niiden korjaamiseksi. (Jaakohuhta & Lahtinen 1997, 498.)

2.1.2 Käytön hallinta

Monissa liikeyrityksissä organisaation yksiköitä tai jopa yksittäisiä projekteja laskutetaan verkon palvelujen käytöstä. Tällainen laskutus on usein sisäistä laskutusta, mutta se kuitenkin sisältää tärkeää tietoa sekä laskuttajalle että laskutettavalle. Vaikka yrityksessä ei olisikaan tällaista laskutuskäytäntöä, on verkon ylläpitäjän pystyttävä seuraamaan verkon resurssien käyttöä käyttäjä- tai käyttäjäryhmätasolla. (Jaakohuhta & Lahtinen 1997, 498.)

Käytön hallinnan avulla voidaan seurata verkon resurssien todellista käyttöä. Näin saadaan tietoa, jonka avulla pystytään kohdentamaan verkkoon suunnatut investoinnit oikein. Esimerkiksi verkon laajentamista suunniteltaessa on tärkeää tietää, mitä yhteyksiä ja palveluita todellisuudessa käytetään ja tarvitaan. Käytön hallinta mahdollistaa myös verkosta aiheutuvien kustannuksien jakamisen käytön mukaan. Käytön hallinnan merkitys on viime aikoina korostunut, sillä palvelut, joita tarjotaan verkosta asiakkaille, edellyttävät jonkinlaista laskutusmekanismia. (Jaakohuhta & Lahtinen 1997, 499.)

2.1.3 Kokoonpanon hallinta

Nykyaikaiset tietoverkot koostuvat yksittäisistä laitteista ja alijärjestelmistä, jotka voidaan määritellä tekemään useita eri toimintoja. Verkon ylläpitäjän on kyettävä tunnistamaan verkon eri laitteet ja määrittelemään niiden väliset yhteydet senhetkisiä tarpeita vastaaviksi. Esimerkiksi verkon laajennuksen tai viasta toipumisen yhteydessä on usein tarpeen muuttaa verkon konfigurointia. Suurissa verkoissa on lisäksi tarpeen tietää, mitä laitteita niissä on, jotta voidaan helpommin inventoida yrityksen omaisuutta ja esimerkiksi suunnitella laitteiden päivittämistä uudemmiksi. (Jaakohuhta & Lahtinen 1997, 500–501.)

Kokoonpanon hallinnan tehtävänä on käynnistää ja pysäyttää verkon laitteita. Usein on toivottavaa, että nämä operaatiot voidaan suorittaa halutuille laitteille esimerkiksi tiettyinä aikoina päivästä tai viikosta. Sen tehtäviin kuuluu myös ylläpitää, lisätä ja päivittää laitteiden tilaa koskevia tietoja ja laitteiden välisiä riippuvuuksia. (Jaakohuhta & Lahtinen 1997, 500.)

2.1.4 Suorituskyvyn hallinta

Useimpien tietoliikenneverkkojen laitteet käyttävät hyväkseen verkosta saatavia jaettuja resursseja, ja juuri niiden jakamisen tarve onkin yleensä ollut verkon rakentamisen syynä. Tällaiselle verkon kautta tapahtuvalle toiminnalle on usein kriittistä, että verkon suorituskyky on riittävällä tasolla. Tämän selvittämiseksi on tarkkailtava verkon laitteita ja arvioitava verkon suorituskyvyn taso. (Jaakohuhta & Lahtinen 1997, 501.)

Suorituskyvyn hallinnan avulla saadaan tietoa verkon eri laitteiden käyttöasteista. Ylläpitäjät tarvitsevat näitä tietoja voidakseen suunnitella, hallita ja ylläpitää suuria verkkoja. Tietoja voidaan käyttää esimerkiksi mahdollisten pullonkaulojen havaitsemiseen. Tällöin voidaan suorittaa ennaltaehkäiseviä toimenpiteitä, ennen kuin pullonkauloista on haittaa loppukäyttäjille. Suorituskyvyn hallinnan avulla siis nähdään, onko tarpeen ryhtyä joidenkin äärirajoilla toimivien resurssien laajentamiseen. (Jaakohuhta & Lahtinen 1997, 502.)

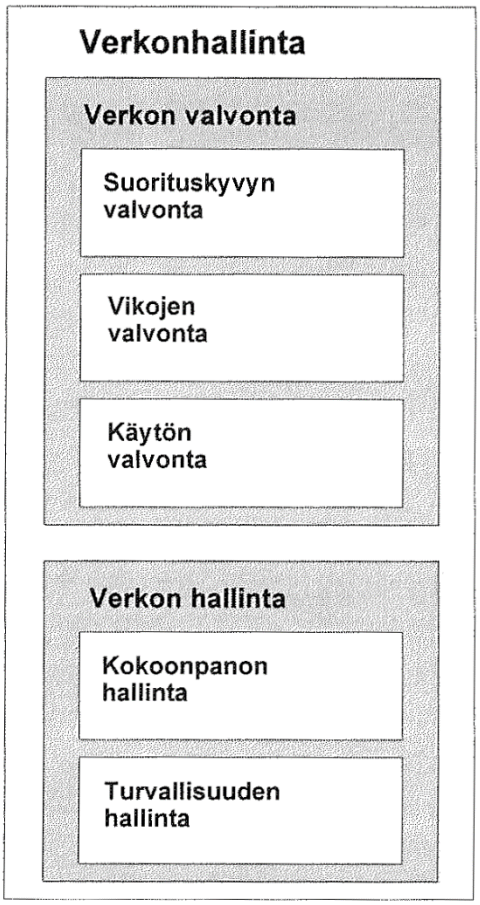
2.1.5 Turvallisuuden hallinta

Turvallisuuden hallinta on verkkoon ja sen laitteisiin pääsyn seurantaa ja tarkastustoimia, sekä pääsyä siihen tietoon, jota on kerätty osana verkonhallintaa. Erilaiset lokeihin kerätyt tiedot ovat tärkeä osa turvallisuuden hallintaa. Siksi turvallisuuden hallinta onkin suurelta osin lokien keräämistä, tallennusta ja analysointia. Turvallisuuden hallinta ei tässä yhteydessä tarkoita järjestelmien sisäistä käyttäjien ja käyttäjäryhmien oikeuksien määrittelyä. Turvallisuuden hallinta keskittyy siihen, kenellä ja mistä on oikeus päästä käsiksi eri laitteisiin ja niistä saataviin palveluihin. (Jaakohuhta & Lahtinen 1997, 503.)

Turvallisuuden hallinta parantaa tietojärjestelmien turvallisuutta. Sen avulla voidaan vähentää murtautumisyrityksiä, kun pääsy laitteisiin ja niiden tarjoamiin palveluihin on sallittu vain tietyistä paikoista. Usein myös pelkkä tieto tehokkaasta turvallisuuden hallinnasta riittää vähentämään murtautumisyrityksiä. (Jaakohuhta & Lahtinen 1997, 504.)

2.2 Verkonhallinnan toteuttaminen

Verkonhallinnan osa-alueet voidaan jakaa kahteen ryhmään: verkon valvontaan ja verkon hallintaan. Valvontaa voidaan pitää verkon kannalta lukuprosessina. Sen avaintehtäviä ovat verkon tilan ja konfiguraation tarkkailu ja analysointi. Verkon hallinta on vastaavasti kirjoitusprosessi. Sen tehtävänä on verkon eri laitteiden asetusten ylläpitäminen. Ohjelmistoa, jolla verkon valvontaa ja hallintaa toteutetaan, kutsutaan verkonhallintajärjestelmäksi. (Jaakohuhta & Lahtinen 1997, 504–505.)



KUVIO 1. Verkonhallinnan jako verkon valvontaan ja verkon hallintaan (Jaakohuhta & Lahtinen 1997, 505)

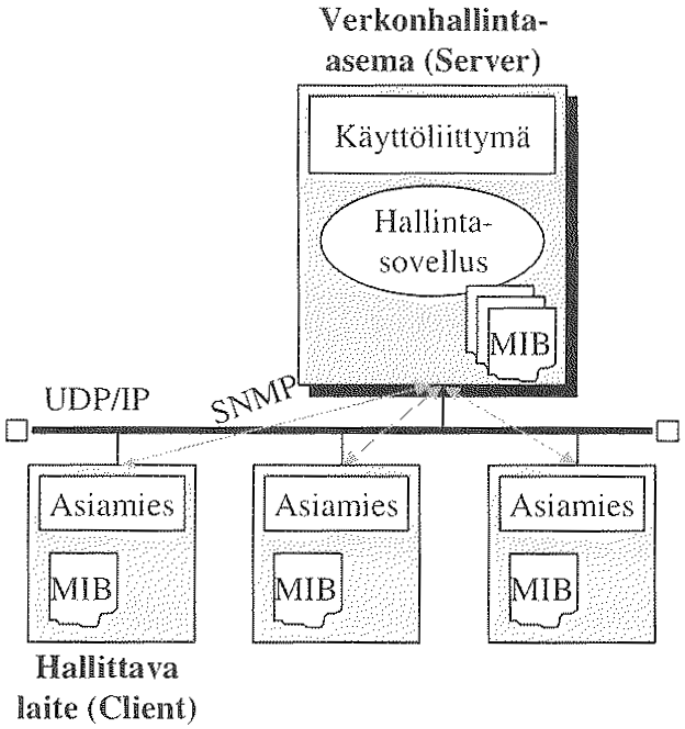
Verkonhallintajärjestelmät käyttävät asiakas-palvelin -protokollia. Verkonhallinta-asema ja hallittavat laitteet vaihtavat käytettävän hallintaprotokollan mukaisia sanomia. Hallituissa asiakaslaitteissa on ohjelmistokomponentti, joka vastaanottaa hallintasanomia ja toimii saamiensa sanomien mukaisesti. Hallinta-asema valvoo laitteiden tilaa, kerää tietoja asiakaslaitteilta ja näyttää hallittavien laitteiden tiedot käyttöliittymässään. Jos asiakaslaite ei vastaa kyselyihin tai kun ylitetään jokin määritelty kynnysarvo, hallinta-asema voi ilmoittaa tästä ylläpitäjälle, kirjata tapahtuman lokiin tai yrittää korjata ongelman automaattisesti esimerkiksi käynnistämällä hallittavan laitteen uudelleen. (Puska 2000, 308.)

3 SNMP

SNMP (Simple Network Management Protocol) on valmistajariippumaton verkonhallintakäytäntö ja yleisin verkonhallinnassa käytetty protokolla. Alun perin SNMP on kehitetty IP-reititinverkkojen hallintaan Yhdysvalloissa vuonna 1988. Siitä on tällä hetkellä kolme versiota, joista ensimmäinen, SNMPv1, on vuodelta 1990. Toinen versio, SNMPv2, on vuodelta 1993. Toistaiseksi uusin versio, SNMPv3, on vuodelta 2002 ja se on yleistymässä edellisiä paremman tietoturvallisuutensa vuoksi. SNMP toimii TCP/IP-protokollaperheen sovelluskerroksella. (Jaakohuhta 2005, 312.)

3.1 SNMP-protokollan toiminta

SNMP on asiakas-palvelin -protokolla. Hallittavissa laitteissa (Managed Network Entity) on SNMP-agentti tai ”asiamies”, joka tarkkailee laitteen tilaa ja raportoi siitä valvojalle. Valvoja on jokin hallintasovellus, joka toimii verkonhallinta-asemassa (Network Management Station). Valvoja pyytää ja kerää kaikkia valvottavia laitteita koskevat tiedot ja tallentaa ne tietokantaansa. (Hunt 1998, 356–357.)



KUVIO 2. SNMP:n asiakas-palvelin -järjestelmä (Puska 2000, 308)

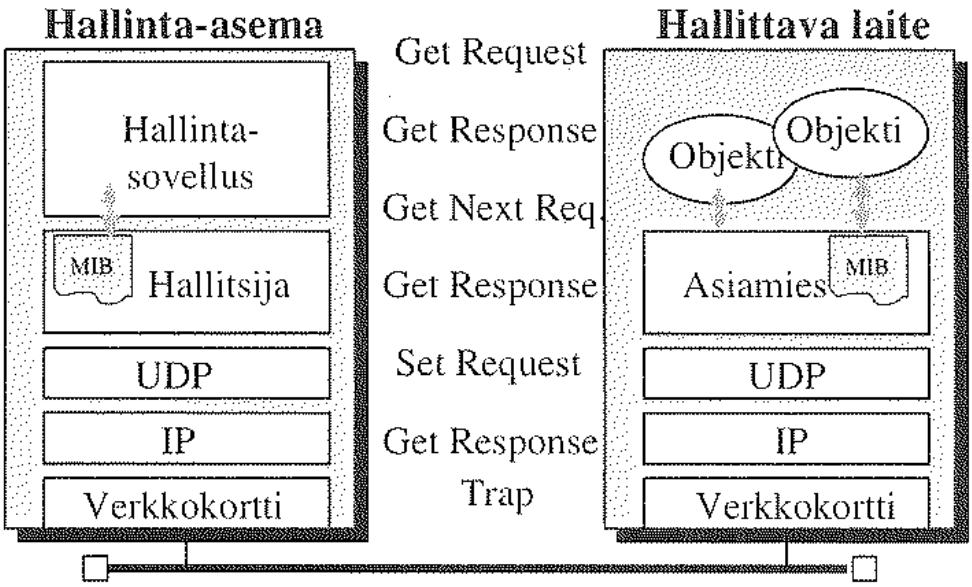
SNMP on kysely-vastaus -protokolla, joka käyttää UDP-portteja 161 ja 162. SNMP käyttää UDP-protokollaa tiedonsiirtoon, koska sen resurssitarve on pienempi kuin TCP:n. TCP-protokollan luotettavuutta ei tarvita, koska jokainen kysely generoi vastauksen. Jos valvoja ei saa vastausta kyselyyn, se lähettää kyselyn uudelleen. Pakettien saapumisjärjestystäkään ei tarvitse valvoa, sillä jokainen kysely ja vastaus käsittää vain yhden tietosähkeen. (Hunt 1998, 357.)

SNMP:n tietosähkeissään lähettämiä kyselyitä ja vastauksia kutsutaan nimellä PDU (Protocol Data Unit). Näiden sanomien avulla valvoja kysyy valvontatiedot ja tarpeen vaatiessa muokkaa niitä. Agentti myös vastaa valvojan kyselyihin ja raportoi epätavallisista tilanteista näiden sanomien avulla. SNMPv1 käyttää viittä erilaista PDU-tyyppiä. (Hunt 1998, 357.)

TAULUKKO 1. SNMPv1:n PDU-sanomat (Hunt 1998, 357)

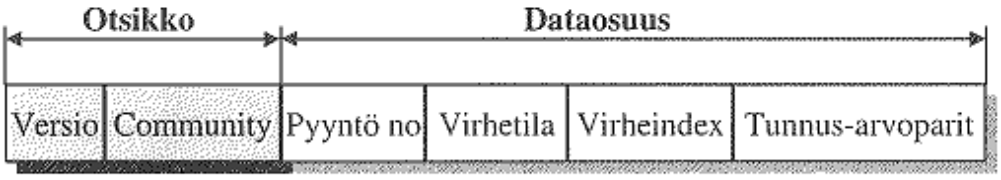
PDU	Käyttö
GetRequest	Valvoja pyytää päivitystietoja
GetNextRequest	Valvoja pyytää seuraavana olevat tiedot
GetResponse	Agentti vastaa valvojan kyselyyn
SetRequest	Valvoja muokkaa hallittavassa laitteessa olevia tietoja
Trap	Agentti lähettää epätavallista tilannetta koskevan sanoman

Valvoja lähettää väliajoin kullekin valvottavalle laitteelle kyselyn (GetRequest) ja jokainen agentti vastaa lähettämällä laitteen tilaa koskevat tiedot (GetResponse). Tällaisia aika ajoin tapahtuvia kyselyitä kutsutaan kiertokyselyiksi (Polling). Kiertokyselyiden heikkous on siinä, että jos valvotussa laitteessa syntyy jokin ongelma, valvoja saa siitä tiedon vasta, kun seuraava kysely lähetetään. Tämän vuoksi SNMP tukee myös tapahtumaohjattua kyselyä (Trap-directed polling). Kun ongelmatilanne syntyy, SNMP-agentti ei jää odottamaan seuraavaa valvojalta tulevaa kyselyä, vaan lähettää epätavallista tilannetta koskevan sanoman (Trap) heti. Nämä sanomat lähetetään valvojalle UDP-porttiin 162. Valvoja lähettää kyselyt valvottaville laitteille porttiin 161. (Hunt 1998, 357.)



KUVIO 3. SNMPv1:n sanomat (Puska 2000, 311)

SNMP-viesti sisältää PDU:n lisäksi otsikon. SNMPv1:n otsikko sisältää versionumeron ja hallinta-alueen nimen (Community name), jolla verkko voidaan jakaa vastuualueisiin ja jota voidaan käyttää heikkoon todennukseen. PDU eli dataosuus sisältää muun muassa pyynnön tyypin ja objektien eli muuttujien arvot. (Puska 2000, 312.)



KUVIO 4. SNMPv1-viestin rakenne (Puska 2000, 312)

3.2 SNMPv2 ja SNMPv3

SNMPv2 lisää protokollaan kaksi uutta PDU:ta. Ensimmäinen niistä on sanoma, jolla hallinta-asema voi lähettää Trap-sanoman toiselle hallinta-asemalle ja pyytää siihen vastausta (InformRequest). Toinen taas on sanoma, jolla hallinta-asema voi ladata suuren määrän tietoa tehokkaasti (GetBulkRequest). SNMPv2 sisältää myös muita parannuksia, mutta se ei täyttänyt kehityshankkeen alkuperäisiä tavoitteita tietoturvan suhteen. SNMPv1:n tavoin SNMPv2:n tietoturvaominaisuudet ovat puutteelliset, koska kaikki sen sanomat lähetetään selväkielisinä ja todennus perustuu vain hallinta-alueen nimeen. (Puska 2000, 311.)

SNMPv3 on kehitetty korjaamaan SNMP-protokollan tietoturvaan liittyvät puutteet. Se on kehitetty SNMPv2:n pohjalta ja siihen onkin lisätty lähinnä vain tietoturvaan liittyviä ominaisuuksia. IETF (Internet Engineering Task Force) on määritellyt SNMPv1:n ja SNMPv2:n jo vanhentuneiksi ja suosittelee nykyään SNMPv3:n käyttöä verkonhallinnassa. (SNMP Research International, Inc. 2015. Viitattu 25.9.2015.)

SNMPv3:n tietoturvaominaisuuksia ovat sanoman todennus ja salaus. Todennuksella varmistetaan, että sanoma on peräisin kelvolliselta lähteeltä. Salauksella taas estetään luvattomia tahoja pääsemästä lukemaan sanomaa. Todennus perustuu MD5- (Message Digest Algorithm 5) tai SHA-algoritmeihin (Secure Hash Algorithm). Salaukseen voidaan käyttää DES- (Data Encryption Standard) tai AES-algoritmeja (Advanced Encryption Standard). SNMPv3:ssa on kolme eri tietoturvatasoa. (Cisco Systems, Inc. 2013. Viitattu 28.9.2015.)

TAULUKKO 2. SNMPv3:n tietoturvatasot (Cisco Systems, Inc. 2013. Viitattu 28.9.2015)

Taso	Todennus	Salaus
noAuthNoPriv	Pelkkä käyttäjänimi	Ei salausta
authNoPriv	Käyttänimi ja salasana (MD5 tai SHA)	Ei salausta
authPriv	Käyttänimi ja salasana (MD5 tai SHA)	DES- tai AES-salaus

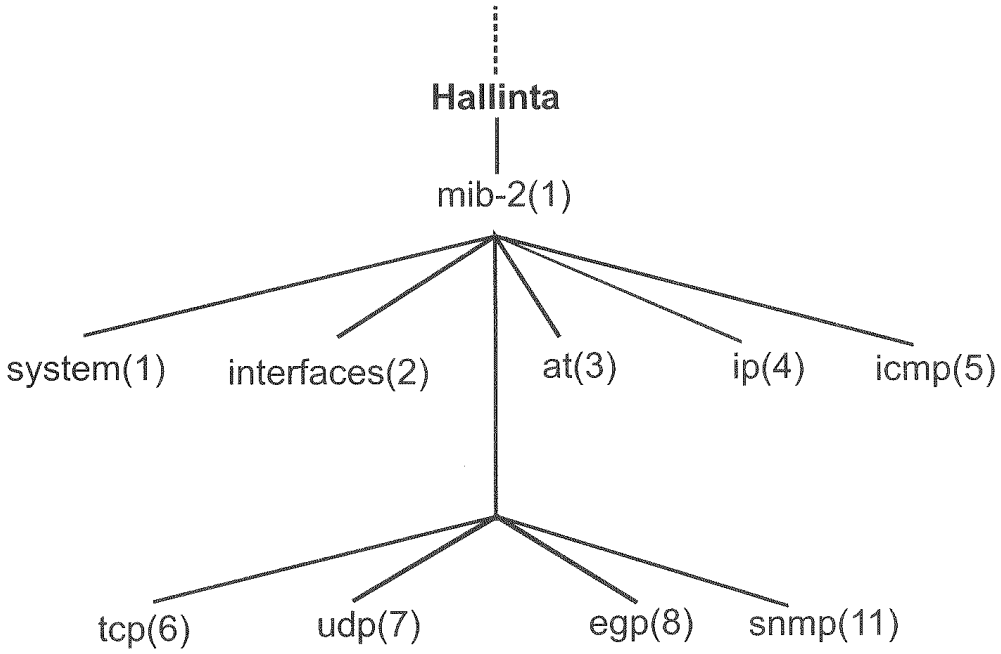
3.3 MIB

MIB (Management Information Base) on pieni tietokanta, joka sisältää tiedot hallittavista laitteista. MIB-tietokanta voi sisältää yleisiä ja toimittajakohtaisia objekteja eli muuttujia, joita tunnetaan yli 1000. Niiden perusteella SNMP hallitsee laitteita. Jokainen objekti kerää tietoa, kuten vastaanotettujen ja lähetettyjen pakettien määriä, ja ylläpitää kerättyä tietoa, jotka agentti sitten välittää verkonhallinta-asemalle. (Jaakohuhta 2005, 315–316.)

Erilaisille laitteille on omat MIB:insa. Standardinmukaisia MIB:eja ovat:

- MIB I yleisille TCP/IP-laitteille
- MIB II Ethernet-, Token Ring- ja FDDI-laitteille
- Hub MIB Ethernet-keskittimille
- Bridge MIB Ethernet-silloille
- Host MIB tietokoneille ja työasemille
- Frame Relay MIB kehysvälitysverkon laitteille
- RMON ja RMON II MIB verkon etävalvontaan
- Manager-to-manager MIB hallinta-asemien väliseen sanomanvaihtoon
  (Puska 2000, 309.)

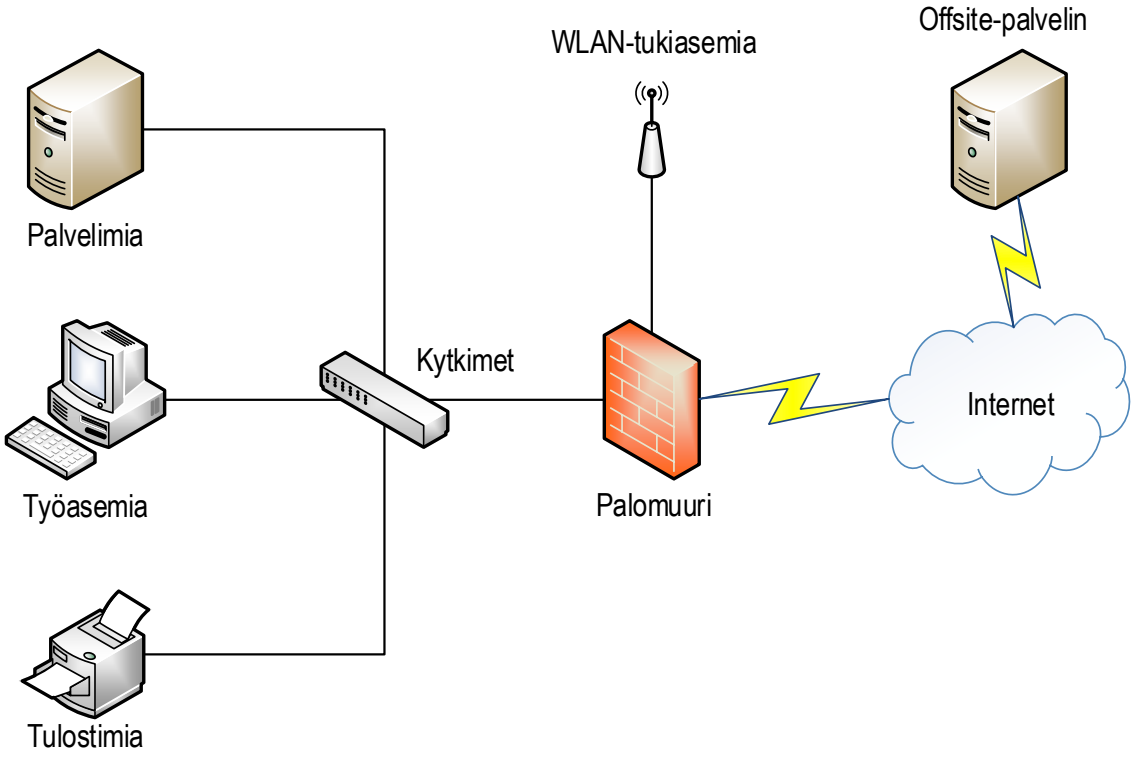
Rakenteeltaan MIB on puumainen. Puun yläosan objektit ovat ISO:n määrittelemiä. Puun alempien tasojen objektit ovat muiden organisaatioiden ja laitetoimittajien määrittelemiä. Puumaista rakennetta kutsutaan SMI:ksi (Structure Management Information). Se tarjoaa työkalut uusien objektien luomiseen ja tunnistamiseen. Objektit voivat sisältää esimerkiksi kokonaislukuarvoja, verkko-osoitteita, laskureita, mittausarvoja, aikaleimoja ja taulukoita. SMI määrittelee myös hierarkkisen nimirakenteen, jolla hallittavat objektit tunnistetaan. Objektit ovat annettuja nimiä ja sijainteja hierarkkisessa rakenteessa, joilla helpotetaan objektien tunnistamista. SMI:n avulla laitetoimittajat voivat määritellä laitteilleen omia hallintaobjekteja. (Jaakohuhta 2005, 315–316.)



KUVIO 5. Puumaisen MIB:in rakenne (Jaakohuhta 2005, 315)

4 ASENNETTAVAT OHJELMISTOT

Toimeksiantajan verkossa oli noin 100 työasemaa sekä useita Windows- ja Linux-palvelimia, joista yksi sijaitsi yrityksen lähiverkon ulkopuolella palvelinhotellissa. Verkossa oli lisäksi palomuuri, kytkimiä, tulostimia, WLAN-tukiasemia ja lukuisia muita laitteita. Verkossa olevien laitteiden määrä oli myös jatkuvasti kasvussa ja näinkin suurta verkkoa oli jo vaikea valvoa pelkästään ihmisvoimin. Yrityksessä oli siis tarve automatisoidulle järjestelmälle, jonka avulla verkossa olevien laitteiden tilaa voitaisiin valvoa ja pitää laitteista kirjaa. Valvontajärjestelmä haluttiin luonnollisesti toteuttaa mahdollisimman pienillä kustannuksilla, joten päätettiin käyttää maksuttomia avoimen lähdekoodin ratkaisuja.



KUVIO 6. Toimeksiantajan tietoverkko

4.1 Observium

Käytettäväksi verkonhallintaohjelmistoksi oli ennakkoselvitysten perusteella valittu Observium. Observium on valvontaohjelmisto, joka kerää tietoa verkon laitteista SNMP-protokollan avulla, tallentaa tiedot tietokantaansa ja näyttää ne web-käyttöliittymässään. Observium toimii suurelta osin automaattisesti ja vaatii vain ylläpitoa. (Observium Limited 2015. Viitattu 2.10.2015.)

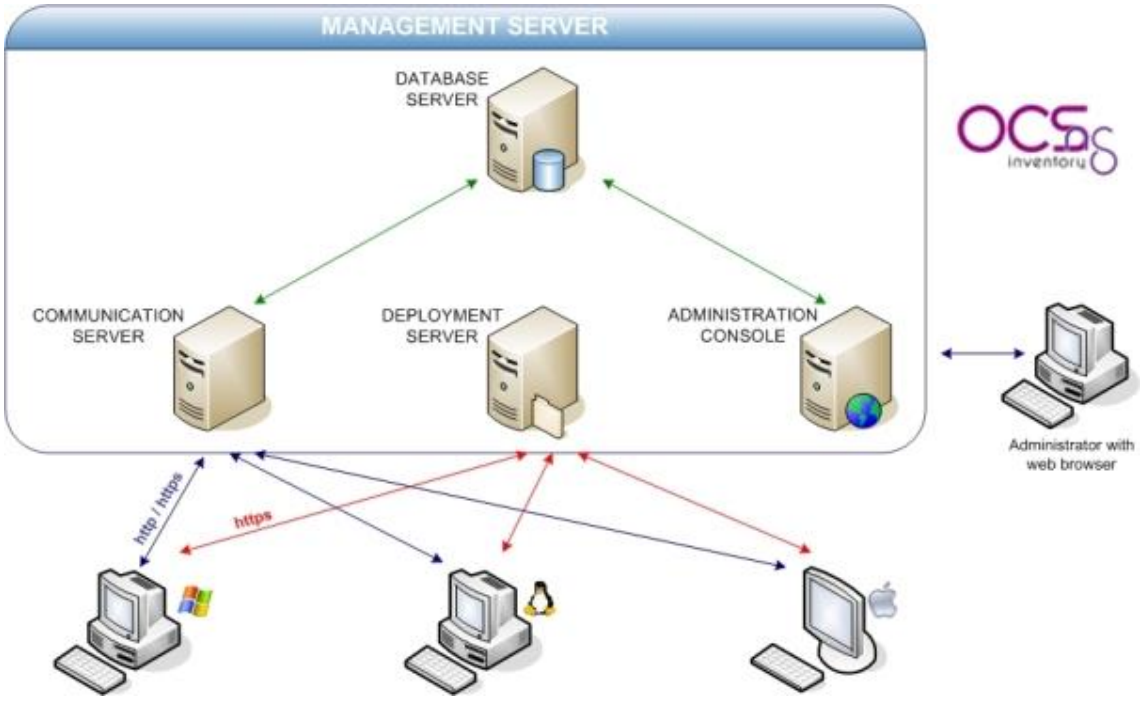
Observium tukee useita erilaisia laitteita ja käyttöjärjestelmiä. Tuettuna on yli 100 yleistä ja toimittajakohtaista MIB-tietokantaa. Observiumilla voidaan valvoa muun muassa reitittimiä, kytkimiä, WLAN-tukiasemia, palomuureja, tulostimia ja UPS-laitteita lukuisilta eri valmistajilta, kuten Cisco, HP, Dell, Juniper ja Palo Alto. Observiumin avulla voidaan valvoa myös Windows- ja Linux-työasemia sekä -palvelimia. Observiumia käyttävät monet suuret Internetissä toimivat yritykset, kuten Twitch, eBay, PayPal ja Spotify. (Observium Limited 2015. Viitattu 2.10.2015.)

Observiumista on kaksi versiota: maksuton Community-versio ja 150 puntaa vuodessa maksava Professional-versio. Community-versiolle julkaistaan päivityksiä kuuden kuukauden välein. Professional-versiolle taas julkaistaan korjauksia ja päivityksiä reaaliajassa. Professional-versiossa on lisäksi ominaisuuksia, jotka Community-versiosta puuttuvat. Threshold Alerting on Professional-version ominaisuus, joka on suunniteltu vikojen hallintaan. Sen avulla laitteille voidaan määritellä kynnysarvoja, joiden ylittyessä Observium ilmoittaa siitä ylläpitäjälle esimerkiksi sähköpostilla. Traffic Accounting taas on ominaisuus, joka helpottaa käytön hallintaa. Sen avulla verkon käyttöä voidaan seurata ja laskuttaa asiakkaita käytön perusteella. Professional-versiolle on lisäksi saatavilla maksullisia tuki- ja palvelupaketteja. (Observium Limited 2015. Viitattu 2.10.2015.)

4.2 OCS Inventory NG

Observiumin lisäksi verkonhallinta-asemaan asennetaan OCS Inventory NG (Open Computers and Software Inventory Next Generation). Se on maksuton ohjelmisto, jonka avulla voidaan pitää kirjaa verkossa olevista tietokoneista sekä niiden laitteistoista ja asennetuista ohjelmista. Kerättyjä tietoja tarkastellaan web-käyttöliittymästä. OCS Inventory NG:n avulla on myös mahdollista jakaa ja asentaa ohjelmia verkossa oleviin tietokoneisiin. (OCS Inventory Team 2014. Viitattu 6.10.2015.)

OCS Inventory NG käyttää omaa työasemiin asennettavaa agenttiaan (OCS Inventory Agent), joka kerää tiedot työasemasta ja lähettää ne väliajoin hallinta-asemalle. Viestintä agenttien ja hallinta-aseman välillä tapahtuu HTTP- tai HTTPS-protokollan avulla. Kerätty tieto on XML-muotoista ja se vielä pakataan verkon liikenteen vähentämiseksi. OCS Inventory NG:n hallintaohjelmisto koostuu neljästä komponentista, jotka kaikki voidaan asentaa myös samaan palvelimeen. Vasta kun inventoitavia tietokoneita on yli 10 000, on suositeltavaa käyttää kahta erillistä palvelinta. (OCS Inventory Team 2014. Viitattu 6.10.2015.)



KUVIO 7. OCS Inventory NG:n viestintäarkkitehtuuri (OCS Inventory Team 2014. Viitattu 6.10.2015)

4.3 LAMP

Sekä Observium että OCS Inventory NG sisältävät web-käyttöliittymän ja siksi ne täytyy asentaa web-palvelimeen. Tässä tapauksessa käytettiin LAMP-ympäristöä. Lyhenne LAMP tulee alun perin sanoista Linux, Apache, MySQL ja PHP. Lyhennettä käytetään kuvaamaan yleistä web-palvelimen kokoonpanoa, jossa palvelimen käyttöjärjestelmänä on Linux, web-palvelinohjelmistona Apache, tietokantaohjelmistona MySQL tai MariaDB ja vuorovaikutteisuuden mahdollistavana ohjelmointikielenä PHP, Perl tai Python. (Linux.fi 2014. Viitattu 5.10.2015.)

Verkonhallinta-asemaan asennettavaksi Linux-jakeluksi oli valittu Red Hat Enterprise Linuxin (RHEL) lähdekoodeihin pohjautuva CentOS (Community Enterprise Operating System). Itseasiassa CentOS on RHEL:n klooni, josta on vain poistettu Red Hatin logot ja tavaramerkit. Tästä syystä pakettien, jotka ovat RHEL-yhteensopivia, voidaan olettaa toimivan myös CentOS:n kanssa. CentOS käyttää RPM-paketinhallintaa ja sen pääasiallisena paketinhallintaohjelmana toimii YUM (Yellowdog Updater Modified). CentOS pyrkii tarjoamaan yritystason käyttöjärjestelmän maksuttomasti. Se soveltuu hyvin palvelinkäyttöön, koska sitä pidetään erityisen vakaana ja luotettavana. Sen jokainen merkittävä versio saa ilmaisia tietoturvapäivityksiä jopa kymmenen vuoden ajan julkaisusta. (DistroWatch 2015. Viitattu 1.10.2015.)

Asennettavaksi CentOS:n versioksi valittiin CentOS 6.7. Uudemman CentOS 7:n käyttämistä harkittiin myös, mutta sekä Observium että OCS Inventory NG toimivat CentOS 6:n kanssa ja tarjoavat verkkosivustoillaan hyvät ohjeet asennukseen. CentOS 7:ssa on tapahtunut jonkin verran muutoksia ja niiden myötä asennusohjeet eivät välttämättä enää pidä paikkaansa. Lisäksi CentOS 6 oli jo ennestään käytössä muissa yrityksen Linux-palvelimissa.

5 TOTEUTUS

Valvontajärjestelmän toteuttaminen aloitettiin luomalla yrityksen Hyper-V -palvelimelle uusi virtuaalikone. Tästä virtuaalikoneesta tehtiin hallinta-asema, johon asennettiin CentOS, Observium ja OCS Inventory NG. CentOS asennettiin käyttäen Minimal ISO -tiedostoa, jotta asennuksesta saatiin mahdollisimman kevyt. Graafista käyttöliittymää ei asennettu, vaan palvelimen hallinta tapahtui komentoriviltä. CentOS:n asennuksen valmistuttua, sen verkkoasetukset konfiguroitiin ja asennettiin päivitykset. Yrityksen DNS-palvelimelle luotiin uutta palvelinta vastaava A-tietue. Jatkossa palvelinta hallittiin SSH-yhteydellä. Hallinta-asemaan asennettiin myös Hyper-V Linux Integration Services, joka parantaa Hyper-V -virtuaalikoneen ja asennetun Linux-jakelun yhteensopivuutta.

5.1 Observiumin asennus

Observiumin asennuksessa noudatettiin Observiumin verkkosivustolta löytyvää asennusohjetta. Ensimmäisenä asennettiin Observiumin edellyttämät paketit, kuten Apache, MySQL ja PHP. Kaikkia tarvittavia paketteja ei löytynyt CentOS:n omasta repositoriosta, joten osa niistä oli asennettava EPEL- (Extra Packages for Enterprise Linux) ja RPM Forge -repositorioista. Itse Observiumista ladattiin viimeisin Community-version asennuspaketti wget-ohjelman avulla. Asennuspaketti oli tar.gz-muodossa ja se purettiin Observiumia varten luotuun hakemistoon /opt/observium. Tänne luotiin myös uudet kansiot, joihin Observium tallentaa lokinsa ja laitteiden tiedoista piirtämänsä graafit.

Seuraavaksi luotiin MySQL-tietokanta, johon Observium tallentaa keräämänsä tiedot. Observiumin konfiguraatiotiedosto config.php muokattiin uutta tietokantaa vastaavaksi. Sinne määriteltiin luodun tietokannan nimi, käyttäjä ja salasana. RHEL-pohjaisessa järjestelmässä tähän tiedostoon täytyi tehdä myös muita pieniä muutoksia, ja poistaa käytöstä SELinux.

Observiumille luotiin käyttäjä, joka pääsee salasanallaan kirjautumaan web-käyttöliittymään. Tämä tapahtui Observiumin asennushakemistosta löytyvän skriptin avulla. CentOS:n cron-ajastuspalveluun määriteltiin samasta hakemistosta löytyvät skriptit, jotka suoritetaan tietyin väliajoin. Näiden skriptien avulla Observium pyytää tiedot kaikilta valvottavilta laitteilta. Apachen httpd.conf-tiedostoon lisättiin VirtualHost-lohko, jossa määriteltiin muun muassa palvelimen nimi ja hakemisto, josta Observiumin web-käyttöliittymä löytyy. Lopuksi CentOS:n iptables-palomuuria konfiguroitiin siten, että sallittiin HTTP-liikenne palvelimelle.

```
<VirtualHost *:80>
   DocumentRoot /opt/observium/html/
   ServerName obsrv.yritys.fi
   CustomLog /opt/observium/logs/access_log combined
   ErrorLog /opt/observium/logs/error_log
   <Directory "/opt/observium/html/">
     AllowOverride All
     Options FollowSymLinks MultiViews
   </Directory>
</VirtualHost>
```

KUVIO 8. Observiumin VirtualHost-lohko

5.2 OCS Inventory NG:n asennus

Observiumin tapaan OCS Inventory NG tarjoaa verkkosivustollaan ohjeen asennukseen. OCS Inventory NG:tä varten täytyi myös asentaa tiettyjä paketteja, joista osa olikin jo asennettu Observiumin yhteydessä. Varsinainen asennuspaketti ladattiin OCS Inventory NG:n verkkosivustolta ja siirrettiin palvelimelle SFTP-yhteydellä. Purettu paketti sisälsi setup.sh-skriptin, jonka avulla asennus sujui suurelta osin automaattisesti. Skripti loi Apachen conf.d-hakemistoon tiedostot, joissa on määritelty muun muassa OCS Inventory NG:n web-käyttöliittymän sijainti /usr/share/ocsreports. Web-käyttöliittymään otettiin yhteys selaimella ja sen kautta luotiin uusi MySQL-tietokanta, johon OCS Inventory NG tallentaa työasemista kerätyt tiedot.

KUVIO 9. MySQL-tietokannan luonti OCS Inventory NG:n web-käyttöliittymästä

5.3 HTTPS-protokollan käyttöönotto

Yhteys Observiumin ja OCS Inventory NG:n web-käyttöliittymiin haluttiin ottaa HTTP-protokollaa turvallisemman HTTPS-protokollan avulla. Tätä varten palvelimeen asennettiin paketit mod_ssl ja OpenSSL. OpenSSL:n komennoilla luotiin hallinta-aseman yksityinen avain ja CSR (Certificate Signing Request). CSR kopioitiin yrityksen sertifikaattipalvelimelle, joka loi sen perusteella sertifikaatin hallinta-asemalle. Yksityinen avain ja luotu sertifikaatti siirrettiin oikeisiin kansioihin hallinta-asemassa.

Apachen httpd.conf-tiedostosta siirrettiin Observiumin VirtualHost-lohko Apachen ssl.conf-tiedostoon. VirtualHost-lohkoon lisättiin SSLEngine-rivi sekä yksityisen avaimen ja sertifikaatin sijainnit palvelimella. Httpd.conf-tiedostoon lisättiin Rewrite-rivit, joiden avulla valvontaohjelmistojen web-käyttöliittymiin tuleva liikenne ohjataan aina SSL-suojatuille sivuille. CentOS:n iptables-palomuuria konfiguroitiin vielä siten, että sallittiin myös HTTPS-liikenne palvelimelle.

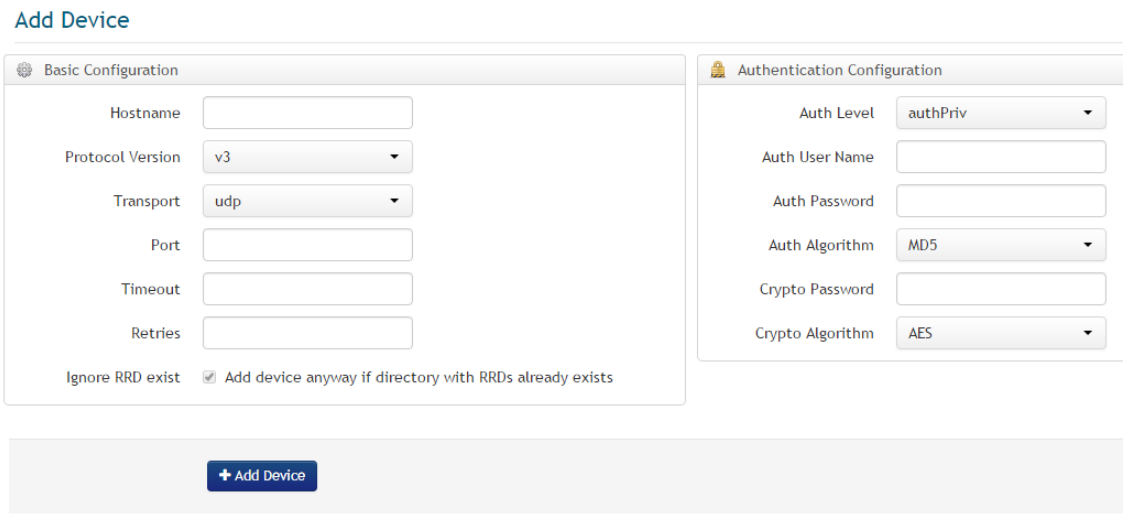
```
RewriteEngine On
RewriteCond %{HTTPS} !=on
RewriteRule ^/?(.*) https://obsrv.yritys.fi/$1 [R,L]
```

KUVIO 10. Rewrite-rivit Apachen httpd.conf-tiedostossa

5.4 Laitteiden lisääminen Observiumiin

Observium valvoo laitteita automaattisesti, mutta ne täytyy ensin lisätä valvottaviksi joko web-käyttöliittymän tai komentorivin kautta. Observiumille täytyy kertoa laitteen nimi (Hostname) ja valita käytettävä SNMP:n versio. Observium ei löydä laitteita IP-osoitteen perusteella, joten DNS-palvelimelta on löydyttävä jokaista valvottavaa laitetta vastaava A-tietue. Osa laitteista löytyikin jo yrityksen DNS-palvelimelta ja puuttuvat lisättiin sinne tässä vaiheessa.

Kaikki valvottavat laitteet käytiin läpi ja asetettiin käyttämään SNMPv3:a, jos laitteesta löytyi sille tuki. SNMPv3:n tietoturvatasoista valittiin turvallisin, authPriv. Tämä edellytti sitä, että laitteisiin oli asetettava todennusta varten käyttäjänimi ja salasana sekä salaukseen käytettävä erillinen salasana. Kun laitteet oli lisätty valvottaviksi, Observium alkoi keräämään niistä tietoa ja piirtämään graafeja esimerkiksi niiden porttien liikennemääristä sekä prosessorin ja muistin käyttöasteista.



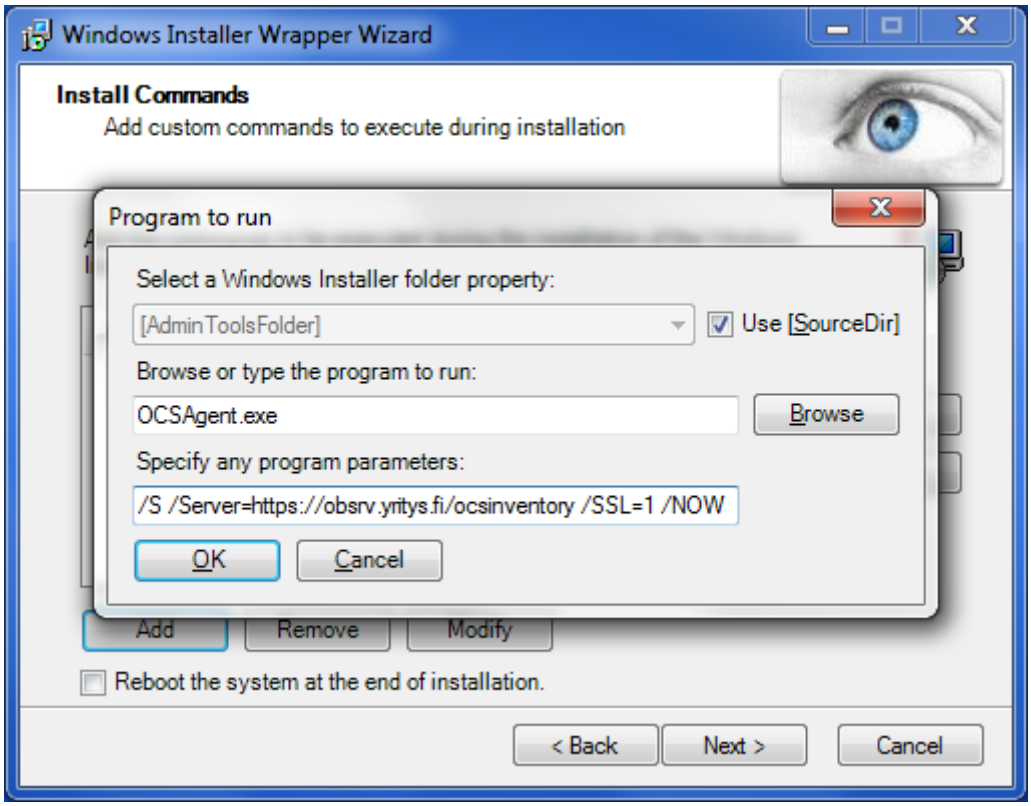
KUVIO 11. Valvottavan laitteen lisääminen Observiumin web-käyttöliittymästä

5.5 OCS Inventory Agentin jakelu työasemiin

Yrityksen verkossa oleviin työasemiin täytyi asentaa OCS Inventory Agent, joka lähettää kunkin tietokoneen tiedot hallinta-asemalle. Yrityksessä oli niin paljon työasemia, että agentin asentaminen käsin jokaiseen työasemaan ei ollut järkevää. Agentista päätettiin tehdä MSI-paketti ja jaella se työasemiin yrityksen SCE-palvelimelta (System Center Essentials). OCS Inventory NG:n verkkosivustolta löytyi ohje myös MSI-paketin tekemiseen. Paketin tekemiseen käytettiin 7-zip ja WIWW-ohjelmia (Windows Installer Wrapper Wizard).

OCS Inventory Agentin lähettämien tietojen SSL-suojausta varten tarvittiin yrityksen sertifikaattipalvelimen CA-sertifikaatti (Certificate Authority). Työasemat varmentavat sen avulla hallinta-aseman ”henkilöllisyyden” ennen tietojensa lähettämistä. CA-sertifikaatti muunnettiin vaadittuun pem-muotoon OpenSSL:n komennon avulla. Muunnetusta sertifikaatista tehtiin vielä exe-muotoinen tiedosto (Self-extracting certificate file) 7-zip -ohjelman avulla. OCS Inventory NG:n verkkosivustolta ladattiin uusin OCS Inventory Agentin asennustiedosto OCSAgent.exe. WIWW-ohjelmalla exe-muotoinen sertifikaatti ja agentin asennustiedosto pakattiin samaan MSI-tiedostoon.

Molemmille MSI-paketin tiedostoille annettiin parametreja, joiden mukaan ne asennetaan työasemiin. Agentin parametriksi annettiin /Server, eli hallinta-aseman osoite, johon agentti lähettää työasemasta keräämänsä tiedot. Parametreiksi annettiin myös /SSL=1, jolla SSL-suojaus otetaan käyttöön ja /S eli Silent, joka suorittaa asennuksen ilman kanssakäymistä käyttäjän kanssa. Lisäksi annettiin parametri /NOW, joka lähettää työaseman tiedot hallinta-asemalle ensimmäisen kerran heti agentin asennuksen päätyttyä. Valmis MSI-paketti siirrettiin yrityksen SCE-palvelimelle ja jaeltiin työasemille Windows Updaten kautta.



KUVIO 12. MSI-paketin teko WIWW-ohjelmalla

5.6 Ongelma tietojen vastaanottamisessa

Observiumin ja OCS Inventory NG:n asentaminen samaan palvelimeen osoittautui hieman odotettua ongelmallisemmaksi. Observiumin käyttöliittymä sijaitsi hakemistossa /opt/observium ja OCS Inventory NG hakemistossa /usr/share/ocsreports. Lisäksi OCS Inventory NG ottaa tietokoneiden lähettämät tiedot vastaan ”virtuaalisen” web-sivun /var/www/html/ocsinventory kautta, jota ei oikeasti ole olemassa.

Observiumin VirtualHost-lohkossa määritelty DocumentRoot-rivi aiheutti sen, että tietokoneiden OCS Inventory NG:lle lähettämät tiedot eivät tulleet perille. Vikaa etsittiin ensin muun muassa MSI-paketista ennen kuin sen todellinen syy löytyi. Ongelma ratkesi lopulta kuitenkin melko yksinkertaisesti. OCS Inventory NG:n web-käyttöliittymän konfiguraatiotiedostoon lisättiin Alias-rivi, joka ohjaa tietokoneilta tulevat tiedot oikeaan osoitteeseen.

```
Alias /ocsinventory /var/www/html/ocsinventory

  <Location /ocsinventory>
        order deny,allow
        allow from all
        # If you protect this area you have to deal with http_auth_*
        # AuthType Basic
        # AuthName "OCS Inventory agent area"
        # AuthUserFile "APACHE_AUTH_USER_FILE"
        # require valid-user
        SetHandler perl-script
        PerlHandler Apache::Ocsinventory
  </Location>
```

KUVIO 13. Alias-rivi OCS Inventory NG:n web-käyttöliittymän konfiguraatiotiedostossa

6 POHDINTA

Opinnäytetyön tarkoituksena oli toteuttaa kohdeyritykselle järjestelmä, jonka avulla voitaisiin valvoa sen verkossa olevien laitteiden tilaa ja pitää kirjaa verkon laitteista. Työn toiminnallinen osuus sujui lähes poikkeuksetta suunnitellusti ja yritys sai käyttöönsä toimivan verkonvalvontajärjestelmän, jota ylläpitäjä käyttää päivittäin. Kirjoitushetkellä valvottavia laitteita oli lähes 30 ja valvottavia työasemia yli 80.

Raportin kirjoittaminen sujui myös hyvin ja pysyin aikataulussa. Pääasiallisina lähteinä käyttämäni kirjat olivat melko vanhoja, mutta niiden sisältämä tieto piti edelleen paikkansa. Verkonhallinta käsittää edelleen samoja asioita, vaikka sen toteuttamiseen tarkoitetut työkalut ovat tietenkin kehittyneet vuosien varrella. SNMP-protokolla toimii myös edelleen samalla periaatteella, vaikka siitä on tullut uusia versiota. Uudempien versioiden toiminnasta löytyi tietoa Internetistä.

Minulla oli jo jonkin verran aikaisempaa kokemusta Linuxista palvelinkäytössä. Opinnäytetyön aikana sain syventää tietojani ja taitojani sen parissa. Mielenkiintoni Linuxia ja muita avoimen lähdekoodin ratkaisuja kohtaan kasvoi entisestään. Hakiessani tietoa opinnäytetyöhön, vastaan tuli lukuisia yrityksiä, jotka tarjoavat jopa satoja euroja kuukaudessa maksavia verkonvalvontaratkaisuja. Avoimen lähdekoodin ohjelmistoilla ja yrityksen jo olemassa olevalla laitteistolla saatiin kuitenkin toteutettua juuri halutun kaltainen järjestelmä maksuttomasti.

Työn tekemisen aikana mieleeni tuli muutamia jatkokehitysideoita. Observiumin maksuton Community-versio voitaisiin vaihtaa Professional-versioon. Professional-versio maksaa 150 puntaa vuodessa, joka on mielestäni edullinen hinta. Sen avulla ylläpitäjä saisi tiedon esimerkiksi sähköpostilla heti, kun verkossa tapahtuu jotain epätavallista. Lisäksi hallinta-asemaan voitaisiin asentaa GLPI (Gestionnaire libre de parc informatique). GLPI on OCS Inventory NG:n kanssa toimiva ohjelmisto, jonka avulla voitaisiin muun muassa toteuttaa tikettijärjestelmä ja pitää kirjaa eri ohjelmistojen lisensseistä.

LÄHTEET

Cisco Systems, Inc. 2013. SNMPv3. Viitattu 28.9.2015.
http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/xe-3se/3850/snmp-xe-3se-3850-book/nm-snmp-snmpv3.html

DistroWatch 2015. Top Ten Distributions. Viitattu 1.10.2015.
http://distrowatch.com/dwres.php?resource=major

Hunt, C. 1998. TCP/IP verkonhallinta. Helsinki: Suomen ATK-kustannus.

Jaakohuhta, H. & Lahtinen, T. 1997. Tietoliikenneverkot: Tehokäyttäjän opas. Espoo: Suomen ATK-kustannus.

Jaakohuhta, H. 2005. Lähiverkot – Ethernet. Helsinki: IT Press.

Linux.fi 2014. LAMP. Viitattu 5.10.2015.
http://www.linux.fi/wiki/LAMP

Observium Limited 2015. Network monitoring with intuition. Viitattu 2.10.2015.
http://www.observium.org/

OCS Inventory Team 2014. Welcome to OCS Inventory NG. Viitattu 6.10.2015.
http://www.ocsinventory-ng.org/en/

Puska, M. 2000. Lähiverkkojen tekniikka. Helsinki: Satku.

SNMP Research International, Inc. 2015. SNMPv3 White Paper. Viitattu 25.9.2015. http://www.snmp.com/snmpv3/v3white.shtml